TW473664

Device, system and method for data access control

Abstract

A device, a method and a system for providing control of access to data which is stored in an electronic data storage device. The device, method and system enable various types of permissions to be set for determining access to the stored data, such that if an attempt is made to access particular data which does not have a suitable permission type, access is denied. Preferably, the present invention is implemented as an access control device, such as a chip for example, which more preferably controls all access to the data storage device. This implementation is preferred, since such electronic devices are more difficult to "hack" for access by an unauthorized user. The device, system and method have a number of different utilizations, such as for controlling access to credit card information; for identifying a user according to a PIN or other identification information; for controlling access to a particular location according to the identity of the user; and for controlling access to various types of data files, such as music files in the MP3 format and so forth.

TW480397

Secure memory

Abstract

A flash memory is secured by disabling write access to the device, thereby preventing unauthorized updating or tampering of the contents. A cryptoengine is included in an integrated circuit (IC) with the flash memory. An attempt to write to the flash memory is successful only if a received encrypted certificate is authenticated by the cryptoengine. If not authenticated, the write enable signal line and the power applied to the flash memory are disabled.

TW470889

Computer system and contents protecting method

Abstract

The present invention relates to a computer system and contents protecting method using the same. When using recording media (116, 117) having medium ID, a secure manager (112) manages enciphering/decoding of contents while using these medium ID. On the other hand, when using an HDD (115) having no medium ID, the secure manager (112) acquires a device ID peculiar to a system through a BIOS and manages enciphering/decoding of

contents recorded on the HDD while using the device ID. The device ID is stored in a safe area inside a computer system. Accordingly, it is able to utilize and protect digital contents by protecting the contents from illegal use even when these contents are recorded on an open recording medium such as hard disk drive.

TW432283

Secure application card for sharing application data and procedures among a plurality of microprocessors

Abstract

An application memory card system includes a secure memory card which can be operatively connected to communicate with a host mainframe microprocessor or hand held device host microprocessor via a standard interface. The secure memory card contains an application processor and an access control microprocessor (ACP), each of which connect through an internal bus to a number of non-volatile addressable memory chips, each organized into a plurality of blocks. Each microprocessor has an additional control signal line included in a control bus portion of its bus for specifying "Execute" access. An access discrimination logic unit which connects to the internal bus and to the non-volatile memory includes an access by type memory writable by the application processor under the control of the ACP for maintaining security. The access discrimination logic unit combines the "Execute" control access signal from a microprocessor with a signal designating the microprocessor source (e.g. external or internal) to define the type of memory access requested and transfers a control enabling signal as a function of the state of the selected stored access control bit indicating if the requested access is allowed to the addressed block.